CLAIMS

1. A contents recording and reproducing apparatus comprising:

a recording and reproducing unit which performs a record and a reproduce of a recording medium, in which the recording medium records a title key file registering therein at least one of a title key which encrypts each of plural title contents corresponding to a program video or sound, and title contents encrypted by the title key;

a key file generating unit which generates at least one of the title key file and registers at least one of the title key in the generated title key file;

a random number generating unit which generates a random number corresponding to each of the plural title key files; and

a TKF random number generating unit which generates a TKF random number for encrypting other title key file associated with the title key file,

wherein the recording and reproducing unit records a set of the title key file generated and the random number in the recording medium, and

the key file generating unit registers the random number corresponding to the title key file, the TKF random number corresponding to the title key file, and an encrypted title key, where the encrypted title key is formed by encrypting the title key with the random number registered in the title key file and with the TKF random number registered in the other title key file.

2. The apparatus according to claim 1, wherein a first title key file is associated with a third title key file, a second title key file is associated with the first title key file, the third title key file is associated with the

second title key file ,and

the key file generating unit further registers a first encrypted title key, the random number and the TKF random number each corresponding to the first title key file, where the first encryption title key is formed by encrypting the title key with the random number registered in the first title key file and the TKF random number registered in the third title key file, registers a second encrypted title key, the random number and the TKF random number each corresponding to the second title key file, where the second encryption title key is formed by encrypting the title key with the random number registered in the second title key file and the TKF random number registered in the first title key file, and registers a third encrypted title key, the random number and the TKF random number each corresponding to the third title key file, where the third encryption title key is formed by encrypting the title key with the random number registered in the third title key file and the TKF random number registered in the second title key file.

3. The apparatus according to claim 1, wherein a first title key file is associated with a second title key file, the second title key file is associated with the first title key file,and

the key file generating unit further registers a first encrypted title key, the random number and the TKF random number each corresponding to the first title key file, where the first encryption title key is formed by encrypting the title key with the random number registered in the first title key file and the TKF random number registered in the second title key file, and registers a second encrypted title key, the random number and the TKF

random number each corresponding to the second title key file, where the second encryption title key is formed by encrypting the title key with the random number registered in the second title key file and the TKF random number registered in the first title key file.

4. The apparatus according to claim 1 further comprising:

a decrypting unit which decrypts the encrypted title key registered in the title key file by using the random number being registered in the title key file read by the recording and reproducing unit, and the TKF random number being registered in the other title key file associated with the title key file,

when a new title key is added to the recording medium, or when the arbitrary title key is deleted from the recording medium;

a re-encrypting unit which generates the encrypted title key by encrypting the decrypted title key with the new random number and the TKF random number registered in the other title key file; and

an updating unit which updates the plurality of title key files by generating the plurality of title key files in which the encrypted title key, the random number, and the TKF random number are registered,

wherein the random number generating unit newly generates the random number registered in each of the plurality of title key files,

the TKF random number generating unit newly generates the TKF random number registered in each of the plurality of title key files, and

the recording and reproducing unit records the plurality of title key files updated by the updating unit in the recording medium.

5. The apparatus according to claim 4, wherein a first title key file is associated with a third title key file, a second title key file is associated with the first title key file, the third title key file is associated with the second title key file , and

the decrypting unit further decrypts the encrypted title key registered in the first title key file by using the random number being registered in the first title key file read by the recording and reproducing unit, and the TKF random number being registered in the third title key file, when a new title key is added to the recording medium, or when the arbitrary title key is deleted from the recording medium, and

the re-encrypting unit generates the encrypted title key in the first title key file by encrypting the title key being registered in the decrypted title key file with the new random number corresponding to the first title key and the new TKF random number corresponding to the third title key file, generates the encrypted title key in the second title key file by encrypting the title key being registered in the decrypted title key file with the new random number corresponding to the second title key and the new TKF random number corresponding to the first title key file, and generates the encrypted title key in the third title key file by encrypting the title key being registered in the decrypted title key file with the new random number corresponding to the third title key and the new TKF random number corresponding to the second title key file.

6. The apparatus according to claim 4, wherein a first title key file is associated with a second title key file, the second title key file is associated with the first

title key file,and

the decrypting unit further decrypts the encrypted title key being registered in the first title key file by using the random number being registered in the first title key file read by the recording and reproducing unit, and the TKF random number being registered in the second title key file, when a new title key is added to the recording medium, or when the arbitrary title key is deleted from the recording medium, and

the re-encrypting unit generates the encryption title key in the first title key file by encrypting the title key being registered in the decrypted title key file with the new random number corresponding to the first title key file and the new TKF random number corresponding to the second title key file,and generates the encryption title key in the second title key file by encrypting the title key being registered in the decrypted title key file with the new random number corresponding to the second title key file and the new TKF random number corresponding to the first title key file.

7. The apparatus according to claim 4, wherein the title key file further registers a generation indicating a version of the title key, and

the updating unit updates the plurality of title key files, when all the generations of the plurality of title key files read by the recording and reproducing unit coincide with each other.

8. The apparatus according to claim 1, wherein the decrypting unit decrypts the encrypted title key being registered in the title key file by using the random number being registered in the title key file existing in the

recording medium, and the TKF random number being registered in the other title key file associated with the title key file, when the arbitrary title key file does not exist or is broken in the plurality of title key files recorded in the recording medium,

the recording and reproducing unit further comprises a recovering unit which recovers the plurality of title key files by generating the plurality of title key files, wherein the plurality of title key files register the encrypted title key being encrypted by the re-encrypting unit, the random number being newly generated by the random number generating unit, and the TKF random number being newly generated by the TKF random number generating unit, and

the recording and reproducing unit records the plurality of title key files recovered by the recovering unit in the recording medium.

9. The apparatus according to claim 8, wherein a first title key file is associated with a third title key file, a second title key file is associated with the first title key file, the third title key file is associated with the second title key file , and

the decrypting unit decrypts the encrypted title key being registered in the third title key file by using the random number being registered in the third title key file existing in the recording medium, and the TKF random number being registered in the second title key file, when the first title key does not exist or is broken in the recording medium, and

the re-encrypting unit generates the encrypted title key in the first title key file by encrypting the title key being registered in the decrypted third title key file with

the new random number corresponding to the first title key file and the new TKF random number corresponding to the third title key file, generates the encrypted title key in the second title key file by encrypting the title key being registered in the decrypted third title key file with the new random number corresponding to the second title key file and the new TKF random number corresponding to the first title key file, and generates the encrypted title key in the third title key file by encrypting the title key being registered in the decrypted third title key file with the new random number corresponding to the third title key file and the new TKF random number corresponding to the second title key file.

10. The apparatus according to claim 8, wherein a first title key file is associated with a second title key file, the second title key file is associated with the first title key file,and

the decrypting unit decrypts the encrypted title key being registered in the second title key file by using the random number being registered in the second title key file existing in the recording medium, and the TKF random number being registered in the first title key file, when the first title key file does not exist or is broken in the recording medium, and

the re-encrypting unit generates the encrypted title key in the first title key file by encrypting the title key being registered in the decrypted second title key file with the new random number corresponding to the first title key file and the new TKF random number corresponding to the second title key file, and generates the encrypted title key in the second title key file by encrypting the title key being registered in the decrypted second title key file

with the new random number corresponding to the second title key file and the new TKF random number corresponding to the first title key file.

11. The apparatus according to claim 8, wherein the title key file further registers a generation indicating a version of the title key, and

the recovering unit recovers the plurality of title key files, when any one of the generations of the plurality of title key files read by the recording and reproducing unit does not coincide with each other.

12. The apparatus according to claim 8, wherein the recording medium includes a protected area incapable of writing an arbitrary value therein, and a user area capable of recording an arbitrary value by an arbitrary application therein,

the recording and reproducing unit records the random number of the title key file in the protected area, records the TKF random number in the user area, and records improper information indicating an improper record as the random number in the protected area when a file except for the title key file is recorded, and

the recovering unit determines whether the improper information is recorded in the random number or not when the encrypted title key is decrypted, and does not recover the plurality of title key files when the improper information is recorded.

13. A method of recording and reproducing contents comprising:

performing a record and a reproduce of a recording medium, in which the recording medium records a title key

file registering therein at least one of a title key which encrypts each of plural title contents corresponding to a program video or sound, and title contents encrypted by the title key;

generating at least one of the title key file and registering at least one of the title key in the generated title key file;

generating a random number corresponding to each of the plural title key files;

generating a TKF random number for encrypting other title key file;

recording a set of the title key file generated and the random number in the recording medium; and

registering the random number corresponding to the title key file, the TKF random number corresponding to the title key file, and an encrypted title key, where the encrypted title key is formed by encrypting the title key with the random number corresponding to the title key file and with the TKF random number corresponding to the other title key file.

14. A computer program product having a computer readable medium including programmed instructions for recording and reproducing contents, wherein the instructions, when executed by a computer, cause the computer to perform:

performing a record and a reproduce of a recording medium, in which the recording medium records a title key file registering therein at least one of a title key which encrypts each of plural title contents corresponding to a program video or sound, and title contents encrypted by the title key;

generating at least one of the title key file and registering at least one of the title key in the generated

title key file;

generating a random number corresponding to each of the plural title key files;

generating a TKF random number for encrypting other title key file;

recording a set of the title key file generated and the random number in the recording medium; and

registering tthe random number corresponding to the title key file, the TKF random number corresponding to the title key file, and an encrypted title key, where the encrypted title key is formed by encrypting the title key with the random number corresponding to the title key file and with the TKF random number corresponding to the other title key file.